CONTINUATION OF APPLICATION FOR A SEARCH WARRANT

1. I, Christopher J. Rodolico, Special Agent (S.A.) of the Federal Bureau of Investigation (FBI), Lansing, Michigan, United States Department of Justice, have been employed as a S.A. of the FBI for over twelve years. During my employment with the FBI, I have conducted investigations into a variety of federal criminal laws, and I have significant experience in enforcement of those laws. I have investigated claims related to online threats as well as numerous violent crimes. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

INTRODUCTION AND PURPOSE OF THE WARRANT

2. I make this continuation in support of an application for a search warrant to search the location identified in Attachment A for evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 115(a)(1)(B) (Influencing, Impeding, or Retaliating Against a Federal Officer) and 18 U.S.C. § 875(c) (Interstate Communication of Threats). These items are more specifically described in Attachment B.

3. As set forth herein, probable cause exists to believe there have been violations of 18 U.S.C. §§ 115(a)(1)(B) and 875(c), originating from Thomas Osamu Matsudo, via Facebook.com posts, and that evidence, contraband, fruits, and instrumentalities of crime are likely to be found at the location identified in Attachment A. The search contemplated by this continuation will include a search for items specified in Attachment B.

4. The search of the vehicles is to include all internal and external compartments and all containers that may contain digital storage devices, or firearms. The search of the

residents present on the property is to locate any digital storage devices on their person that may contain evidence of threatening communications or other information necessary to access evidence of threatening communications found elsewhere. Additionally, persons located on the premises will be searched for weapons that could be used to carry out the threats further described below.

5. I am familiar with the information contained in this continuation based upon the investigation I have conducted and based on information provided to me by other law enforcement officers/intelligence research specialists who have engaged in this investigation.

6. The facts in this continuation come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Since this continuation is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence and instrumentalities of crime in violation of 18 U.S.C. § 115(a)(1)(B) and 18 U.S.C. § 875(c) will be found in the location identified in Attachment A.

FACTUAL BACKGROUND OF INVESTIGATION

7. On December 14, 2020, the FBI Office of Public Affairs (OPA) forwarded to the FBI National Threat Operations Center (NTOC) a comment posted on social media by Facebook username "Tom Matsudo" in which Matsudo makes veiled threats toward FBI employees. As of December 2020, Matsudo was a repeat complainant to FBI NTOC and

had exhibited escalating behavior in many of his comments on posts by the FBI's Facebook page.

8. The FBI's OPA electronically monitors comments directed to the FBI's 60 plus social media accounts (Twitter, Facebook, YouTube etc.) which are managed by FBI Headquarters and Field Offices. If keywords are discovered within a message sent to one of these social media sites that may indicate a threat, a tip is automatically generated and sent to the National Threat Operations Center for a credibility assessment.

9. As of December 2020, Matsudo had made several posts on the FBI Facebook webpage. Many of the posts were rambling and incoherent. Included in those posts were - "DEAD POLICE IS JUSTICE," "Black hat fraud extortion dead police," "I OWN PEPPER SPRAY AND GUNS. EXPECT TO BE FACING THE GUN".

10. An open source review of the Tom Matsudo Facebook page revealed a post in which he provided what appears to be his full name as Thomas O. Matsudo. A subsequent LexisNexis Accurint query for Thomas Matsudo revealed one result for Thomas Osamu Matsudo with date of birth May X, 1991, and a most recent address in Haslett/Lansing, MI. An additional review of NTOC's Threat Intake Process System (TIPS) revealed numerous instances in which Matsudo called NTOC to report information like that he frequently posts on Facebook.com. In each of his calls to NTOC, Matsudo provided his date of birth as May X, 1991 and telephone number as 517-896-1727.

11. On January 4, 2021, Special Agent (S.A.) Andrew DeCoster, interviewed Thomas Osamu Matsudo telephonically. During the interview Matsudo acknowledged he was

the owner of the Facebook.com username "Tom Matsudo" and he resided at 3977 Halter Lane, East Lansing, MI.

12. S.A. DeCoster is known as "Drew" to family and friends and refers to himself as "Drew" during professional contacts also. During the January 4 interview, S.A. DeCoster referenced himself as "Drew" to Matsudo.

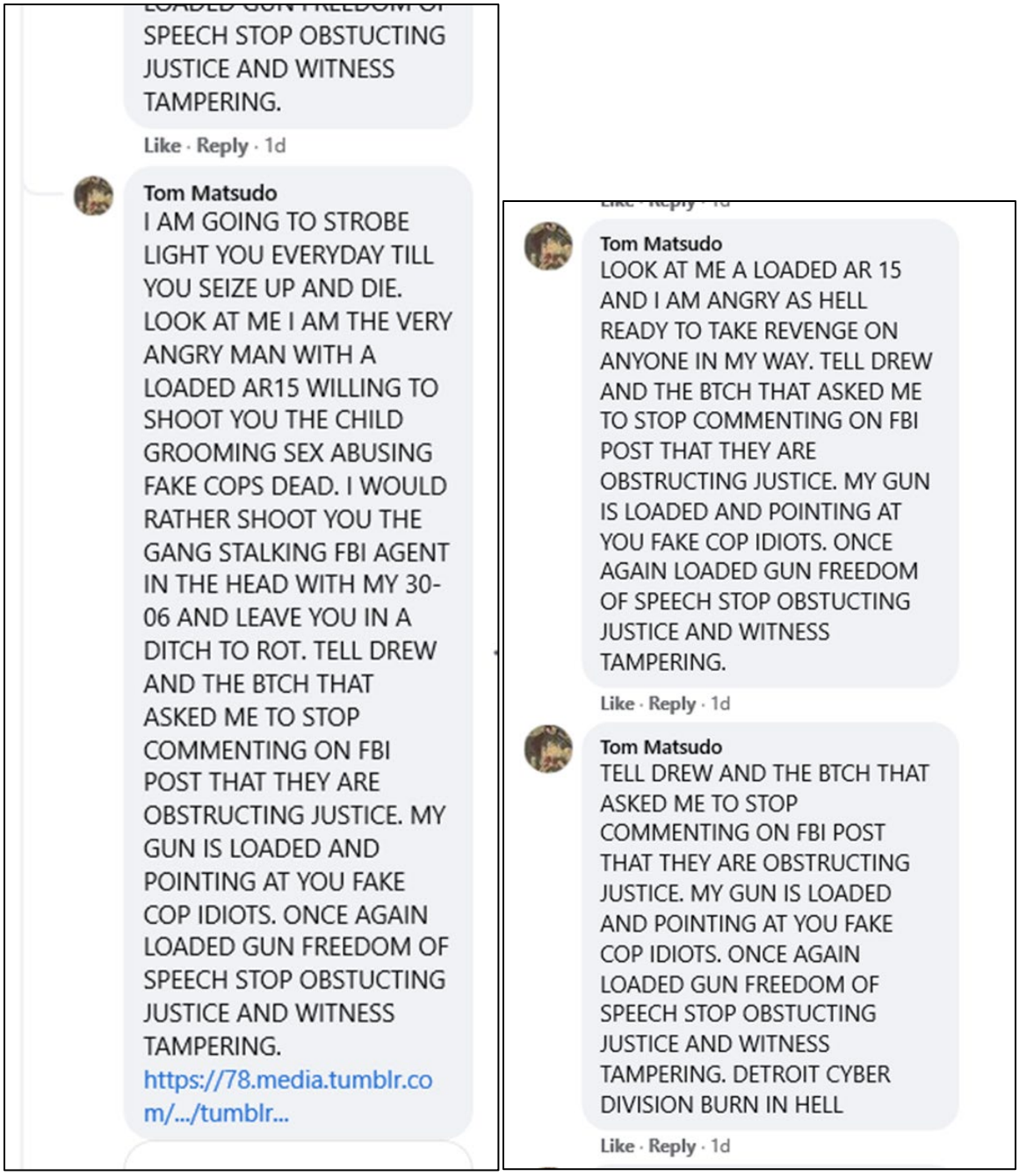
13. In the interview Matsudo stated he purchased a Mossberg (a gun manufacturer known to this Agent) and had seven guns. Matsudo stated he had a Concealed License Permit in Michigan and always carried a Kimber Micro pistol with him.

14. Following the telephonic interview with S.A. DeCoster, Matsudo requested the FBI perform a review of his electronic devices. S.A. DeCoster and FBI S.A. Scott Robinson (also assigned to the East Lansing Resident Agency of the FBI) met with Matsudo, retrieved his electronic devices, had Matsudo sign a consent to search form, and later returned the devices to Matsudo.

15. A Law Enforcement Information Network query showed Matsudo has four pistols registered to himself. Matsudo also has a Concealed License Permit (known as a CPL).

16. On March 27, 2021, S.A. DeCoster received an email from the NTOC regarding a Facebook post made by Thomas Matsudo.

17. On March 29, 2021, I went to FBI's Facebook page and retrieved screenshots of several of Matsudo's posts. These are a few of the screenshots I captured:



18. Between March 27 and March 29, 2021, Matsudo posted approximately 15 times to the FBI Facebook.com page and made five references to "Drew" and the "BTCH that asked me to stop commenting on FBI post."

19. The five aforementioned posts were similar to the above quoted posts with slight variations.

20. On December 21, 2020, Matsudo was issued a speeding ticket from the Meridian Township Police Department, (MI), Matsudo was driving the 2019 Chevrolet Camaro, MI license plate HAWAII1.

21. On March 29, 2021, at approximately 4:09 p.m., FBI S.A. Whitney Mitchell observed a dark-colored Chevrolet Camaro with license plate HAWAII1 in the driveway at 3977 Halter Lane, East Lansing, Michigan.

FACEBOOK

22. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

23. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

24. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

25. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

26. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information

about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

27. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

28. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the

chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

29. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

30. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

31. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

32. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

33. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When

a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

34. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

35. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

36. Information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or

alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or

consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

37. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

COMPUTER SYSTEMS

38. Facebook.com is an internet website and application, and to post to Facebook.com, someone must be connected to the internet.

39. Computers and Internet-capable devices such as tablets and cellular telephones facilitate online posting. Based upon my knowledge, experience, and training, people who post online use computers and handheld devices, such as cellular phones and tablets. The posts/messages can be accessed and traced back to those devices. There is probable cause to believe that a Matsudo used the internet and an electronic device to make these threats and that those computers or online devices will be found in the location identified in Attachment A.

40. Storage capacity of computers and portable storage media, such as USB or thumb drives, has grown tremendously in recent years. These drives can store thousands of data points, are easily transportable, and are relatively inexpensive. Advances in technology have significantly reduced the size of digital storage devices such that now large numbers of digital files can be stored on media that will fit in a person's pocket, on a keychain, or

in any number of easily transportable and concealable places. An individual can now easily carry on his or her person storage media that contains thousands of files.

41. As with most digital technology, communications made from a computer device are often saved or stored on that device. Storing this information can be intentional, for example, by saving an email as a file on the computer or saving the location as a "favorite" website in a "bookmarked" file. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be stored automatically in many places, such as temporary files or Internet Service Provider (ISP) client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files.

42. A forensic examiner often can recover evidence that shows whether a computer device accessed certain web pages. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file often does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten.

43. Similarly, web pages that have been viewed via the Internet are often automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

44. Searches and seizures of evidence from computers and computer devices commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment.

45. To examine the computer and digital media properly, it may also be necessary to seize certain other items including documentation of programs, passwords, notes, or even specialized hardware. Therefore, this warrant seeks permission to seize not only the digital storage media and to search it for evidence

46. The time period required for a complete, safe, and secure forensic examination of the computer and storage media is uncertain. The Government will make available for pick-up within a reasonable time all items found not to contain any contraband or material to be seized pursuant to the warrant and all hardware and software no longer needed for examination purposes. In conducting the search, the forensic examiner and agents will examine files regardless of their name because such names and file extensions

can be altered to conceal their actual content. Because of the volume of data to be searched and the need to complete the examination in a reasonable time, the forensic examiner will also use computer techniques such as keyword searches that may result in the display of irrelevant materials.

47. Because investigators do not know the devices Matsudo used to access the Internet; create, save, access, or hide threats; or communicate with others about threats, investigators may need to preview computer devices to determine which devices might contain evidence listed in Attachment B.

48. Items determined on-scene not to contain items listed in Attachment B will be left at the location identified in Attachment A. The remaining items will be seized and searched for further review or forensic examination and will be returned as soon as reasonably possible if they are determined not to contain evidence listed in Attachment B.

49. Retention of any computers would be warranted, if any online threats are found thereon, in order to permit forfeiture of those computers and related properties as instrumentalities of the crime, pursuant to 18 U.S.C. § 115(a)(1)(B) and 18 U.S.C. § 875(c).

BIOMETRIC ACCESS TO COMPUTER DEVICES

50. The proposed warrant would permit law enforcement to compel MATSUDO to unlock any electronic devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

51. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic

devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

52. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

53. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate

similarly to Trusted Face.

54. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

55. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

56. As discussed, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search

authorized by this warrant.

57. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

58. Due to the foregoing, if law enforcement personnel encounter any electronic devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of MATSUDO to the fingerprint scanner of the devices found; (2) hold the electronic devices in front of the face of MATSUDO and activate the facial recognition feature; and/or (3) hold the devices found in front of the face of MATSUDO and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized

by this warrant. The proposed warrant does not authorize law enforcement to compel that all individuals present to state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel the individuals to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION

59. I respectfully submit that there is probable cause to believe that a search of the location identified in Attachment A will reveal evidence of violations of 18 U.S.C. § 115(a)(1)(B) and/or 18 U.S.C. § 875(c).

60. Wherefore, by this continuation and application, I respectfully request that the Court issue a search warrant that would allow agents to search the location identified in Attachment A for the items listed in Attachment B.